Certification Report

EAL 2+ Evaluation of

EMC® Disk Library v3.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-63-CR
Version: 0.9
Date: 22 January 2008
Pagination: i to v, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 January 2008, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- EMC® is a registered trademark of EMC Corporation,
- Microsoft and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

The EMC® Disk Library v3.1, from EMC Corporation (hereafter referred to as EMC® DL v3.1) was the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The EMC® DL V3.1 is a disk-based backup solution which provides emulated physical tapes that can be used by backup servers connected to a Storage Area Network (SAN). These backup servers are used by an organization to perform backup of corporate user machines or corporate data servers. Since the EMC® DL V3.1 is a disk-based backup solution, it offers significant speed improvements over traditional tape backup. However, since it emulates a traditional tape storage solution, it can be used in conjunction with an organization's existing backup solution. In a typical deployment scenario, the EMC® DL V3.1 is connected to a SAN through one or more Fibre Channel connections. Backup servers are also connected to this SAN to allow them to make use of the EMC® DL V3.1.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 08 January 2008 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the EMC® DL V3.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The Communications Security Establishment, as the CCS Certification Body, declares that the EMC® DL V3.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level EAL 2+ evaluation is the EMC Disk Library v3.1, from EMC Corporation (hereafter referred to as EMC® DL V3.1).

2 TOE Description

The EMC Disk Library provides a disk-based backup solution in a SAN environment. The product ensures that user data is stored securely and is also designed to ensure the integrity of the data that is entrusted to it.

The EMC® DL V3.1 provides the ability for administrators to configure virtual tapes. A virtual tape is the basic unit of storage provided to backup servers. Each virtual tape is created with either a fixed capacity or a variable capacity. The storage provided by the virtual tape exists on the drive storage system provided by the EMC® DL V3.1 and is stored using disks configured in a RAID 5 (Redundant Array Independent/Inexpensive Disks) configuration. RAID 5 provides for data integrity when an individual disk drive fails.

Each virtual tape that is created by an administrator can be assigned to a virtual tape library. A virtual tape library is a collection of virtual tapes. This virtual tape library is also configured to support a certain number of virtual tape drives. Since the EMC® DL V3.1 is designed to emulate traditional tape based backup hardware, the library, drives, and tapes must all be emulated. The virtual tape drive in the EMC® DL V3.1 emulates the interface of a traditional tape drive and allows a backup server to read and write data to a virtual tape.

In addition to grouping together virtual tapes and virtual tape drives, a virtual tape library also is assigned to one or more backup servers. Each backup server is connected to the SAN through a Fibre Channel card. Each Fibre Channel port on a Fibre Channel card has a World Wide Port Name (WWPN) associated with it that is transmitted through the SAN with every data request. Administrators of the EMC® DL V3.1 can configure the access permissions for each virtual tape library based on the backup server WWPN. This allows an administrator to restrict access to the virtual tapes contained within each virtual library to authorized backup servers.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC® DL V3.1 is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature: Title: *EMC Corporation EMC® Disk Library v3.1 Security Target, Version: 1.02, Date: 8 January 2008*.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

The EMC Disk Library v3.1 is:

a. Common Criteria Part 2 conformant; with functional requirements based only upon functional components in Part 2;
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 augmented, with all the security assurance requirements in the EAL 2 package as well as ALC_FLR.1 Basic Flaw Remediation.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication and Security Management. An Administrator must authenticate to the IT Environment before being able to perform any TSF-mediated actions. The TSF enforces the Discretionary Access Control SFP to restrict the ability to configure virtual tapes, virtual tape drives, virtual tape libraries, and administrator access.

Protection of User Data. All user data stored on the TOE is protected by the virtual tapes that have been configured by the Administrator. Access to the virtual tapes is limited to backup servers that have been granted access by the Administrator. Additionally the integrity of the data entrusted to the TOE is ensured through its use of RAID.

For more information on security policy enforcement please refer to the *EMC® Disk Library v3.1 Security Target*.

7 Assumptions and Clarification of Scope

Consumers of the EMC® DL V3.1 product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- There are one or more appropriately trained individuals assigned to manage the EMC® DL V3.1 and the security information it contains; and

- Administrators and TOE users are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security will be provided for the TOE and its environment.

For more information about the EMC® DL V3.1 security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The EMC® DL V3.1 is intended for use by a non-hostile and well-managed user community. It relies on the environment to provide it physical and logical protection.

8 Architectural Information

The TOE is composed of two software components, the *EMC Disk Library* and the *EMC Disk Library Management Console*.

The *EMC Disk Library* provides a disk-based backup solution in a SAN environment. The product ensures that user data is stored securely and is also designed to ensure the integrity of the data that is entrusted to it. The *EMC Disk Library* runs on custom-built hardware developed by EMC Corporation.

The *EMC Disk Library Management Console* handles administration of the EMC® DL V3.1, either through the *EMC Disk Library Management Console* GUI or the *EMC Disk Library Management Console* CLI (Command Line Interface) via a Secure Shell (SSH) connection. Administrators can create and manage virtual tapes, virtual tape drives, and virtual tape libraries through the *EMC Disk Library Management Console* which is installed on a general purpose computer with a Windows Server 2003 SP2 operating system.

9 Evaluated Configuration

The TOE is a purpose-built hardware/software appliance (models DL4100, DL4200, and DL4400), and a software application which runs on a standard PC running Microsoft Windows Server 2003 SP2. EMC® Disk Library v3.1 Build 1549 was tested with the Management Console installed on a standard PC running Microsoft Windows Server 2003 SP2.

10 Documentation

The EMC Corporation documents provided to the consumer are as follows:

a. EMC CLARiiON Disk Library 3.0 Administrator's Guide;
b. EMC Disk Library 3.01 Command Line Interface (CLI) Reference;
c. EMC Disk Library 3.01 Quick Start Guide;
d. EMC Disk Library 3.0 Release Notes; and
e. EMC Disk Library v3.1 Common Criteria Administrative Guide Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EMC Disk Library v3.1, including the following areas:

Configuration management: An analysis of the EMC® DL V3.1 CM system and associated documentation was performed. The evaluators found that the EMC® DL V3.1 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the EMC® DL V3.1 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life cycle: The flaw remediation process was carefully reviewed. There are adequate procedures in place to track and correct security flaws, identify corrective actions, and distribute the flaw information and corrections. A verification of this process was performed during the site visit.

Design documentation: The evaluators analysed the EMC® DL V3.1 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the EMC® DL V3.1 guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The EMC® DL V3.1 ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of

public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2+ consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. These tests focused on:

- Security Management; and
- User Data Protection.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on

- Generic vulnerabilities;
- Bypassing;

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

- Tampering; and
- Direct attacks.

Penetration tests included buffer overflow attacks, data interception attacks, denial of service attacks, and attacks against externally accessible TOE components.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

12.4 Conduct of Testing

The EMC® DL V3.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's Massachusetts facility.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the EMC® DL V3.1 behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the EMC® DL V3.1 in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2+** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The EMC® DL V3.1 is straightforward to configure, use and integrate into a corporate network.

EMC Corporation Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

EWA-Canada performed separate site visits to review developer processes (ACM, ADO, ALC, and ATE) and to repeat a sample of developer's tests. Though development security was not part of the evaluation, the evaluators observed that the developer was exceptionally conscious of security. The physical, procedural, and personnel security measures meet or exceed the assurance requirements of higher-level CC evaluations. This is reported on in the

CC Evaluation Site Visit Report. This document contains proprietary and confidential EMC information.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CC	Common Criteria
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
CSE	Communications Security Establishment
DL	Disk Library
EAL	Evaluation Assurance Level
EMC® DL V3.1	EMC Disk Library
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories Canada
PC	Personal Computer
QA	Quality Assurance
RAID	Redundant Array Independent/Inexpensive Disks
SAN	Storage Area Network
SFP	Security Function Policy
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WWPN	World Wide Port Name

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005; and

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. EMC Corporation EMC® Disk Library v3.1 Security Target, Version 1.02, 8 January 2008.

e. Evaluation Technical Report (ETR) EMC® Disk Library v3.1, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-63, Document No. 1542-000-D002, Version 1.4, 8 January 2008.